Sicherheit im elektronischen Geschäftsverkehr - Rechtsverbindlichkeit durch digitale Signaturen

Vortrag von Dipl.-Inf. Robert Gehring
gehalten am 30. Juni 1998
in Berlin

Übersicht

Hinweis: *Der Leser bzw. die Leserin wird feststellen, daß sich in den einzelnen Abschnitten Hyperlinks befinden, die sich nicht aktivieren lassen. Der Grund dafür ist, daß ich gegenwärtig eine umfangreichere Publikation zum Thema vorbereite, die 1999 erscheinen wird. In diese Publikation ist der untenstehende Vortrag integriert worden. Sollten zum Vortrag Fragen auftauchen, so können diese per Email an mich geschickt werden. Dazu kann der Hyperlink am unteren Ende dieser Seite benutzt werden. Bitte geben Sie in der Betreff-Zeile (subject line) der Email das Stichwort "[IHK]" an. Ich werde mich bemühen, alle Fragen zu beantworten. Die Antworten werden dann im Abschnitt 4 (FAQ's) zu finden sein.*

1. *Meilensteine der historischen Entwicklung*
2. *Symmetrische/asymmetrische Verschlüsselungsverfahren*
3. *Zweck: Daten- und Kommunikationssicherheit*

(3) Grundlagen und Konzepte digitaler Signaturen

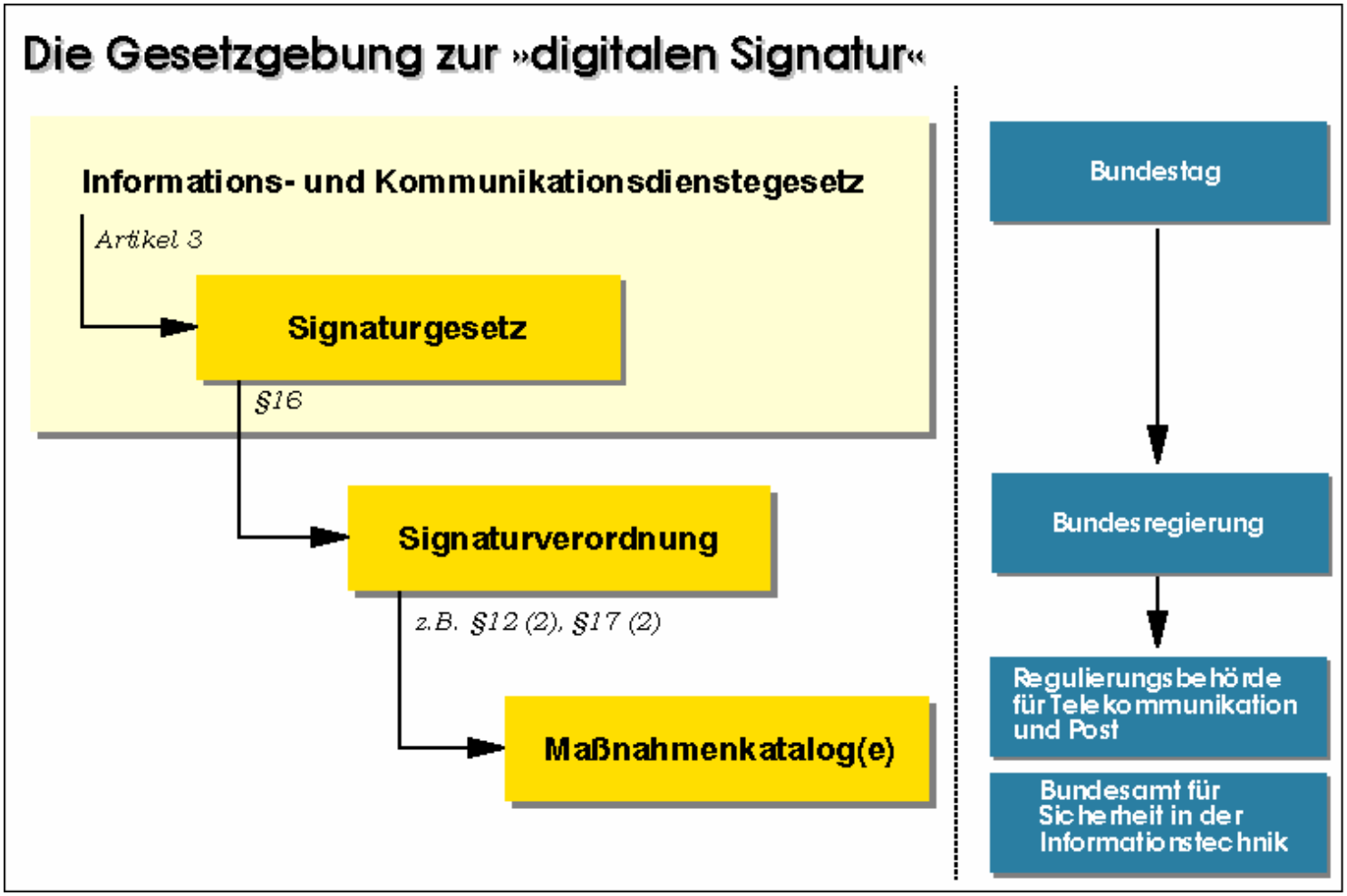
1. *Grundbegriffe: Identität, Integrität, Authentizität, Unabweisbarkeit*
2. *Kryptographische Primitive: Hashfunktionen, Public Key-Verfahren*
3. *Schlüsselverwaltung, Zeit*
4. *Summa summarum: Die digitale Signatur*

(4) FAQ's (Fragen und Antworten)

Zur Eingangsseite

Letzte Änderung: 9. November 1998, Dipl.-Inf. Robert Gehring

(1) Die "Multimediagesetzgebung"



(1.1) Das Informations- und Kommunikationsdienstegesetz (*IuKDG*)

Das IuKDG wurde im Dezember 1996 beschlossen und trat zum 1. August 1997 in Kraft. Es bildet den Rahmen für die gesetzlichen Regelungen, die den Weg in die Informationsgesellschaft vorgeben sollen.

Im IuKDG werden drei neue Gesetze eingeführt:

- Artikel 1: Teledienstegesetz (*TDG*)
- Artikel 2: Teledienstdatenschutzgesetz (*TDDSG*)
- Artikel 3: Signaturgesetz (*SigG*)

Andere Gesetze werden angepaßt, u.a.:

- Artikel 4: Strafgesetzbuch
- Artikel 7: Urheberrechtsgesetz

(1.2) Signaturgesetz (*SigG*), Signaturverordnung (*SigV*), Maßnahmenkatalog

(1.2.1) Das Signaturgesetz (*SigG*)

Zitat

„Zweck des Gesetzes ist es, Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können. "

§1 Abs. 1 SigG

Der Erfüllung dieses Zweckes sollen dienen:

- Vorschriften für Verfahren zur Signaturerzeugung
- Vorschriften zur Zertifizierung
- Lizenzen für Zertifizierungsstellen
- Anforderungen an die Infrastruktur der Zertifizierungsstellen
- Datenschutzregelungen
- Anforderungen an technische Komponenten
- Signaturverordnung

(1.2.2) Die Signaturverordnung (*SigV*)

Die Signaturverordnung beinhaltet die Durchführungsbestimmungen zu den Paragraphen 3 bis 15 des Signaturgesetzes. Dazu gehören im wesentlichen:

- Genehmigungsverfahren für Zertifizierungsstellen
- Vorgaben zur Arbeit der Zertifizierungsstellen
- Festlegung von Bearbeitungskosten

- Ablauf der Zertifizierung
- Regelungen zur Schlüsselverwaltung
- Vorschriften zum Umgang mit Zertifikaten
- Anforderungen an technische Komponenten: *Maßnahmenkatalog(e)*
- Bestimmung des BSI als Prüfinstanz

(1.2.3) Der Maßnahmenkatalog

Der Maßnahmenkatalog wird von der Regulierungsbehörde für Telekommunikation und Post (RegPT) vorgelegt und durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Zusammenarbeit mit Experten aus Wirtschaft und Wissenschaft erarbeitet.

Der Katalog enthält die im Signaturgesetz referenzierten einzelnen Maßnahmenkataloge zur Ausgestaltung von Zertifizierungsstellen, Signaturkomponenten, kryptographischen Verfahren usw.

Beispiel (Zitat aus dem Maßnahmenkatalog):

Zitat

„Die Zertifizierungsstelle muß ein Schlüsselpaar, bestehend aus öffentlichem und privatem Schlüssel, erzeugen, welches mit dem gewählten Verfahren zur Bildung digitaler Signaturen korrespondiert. Dieses Schlüsselpaar wird für die Zertifizierung der öffentlichen Schlüssel der Teilnehmer benötigt, die an dem Verfahren für digitale Signaturen teilnehmen, das von der ZS unterstützt wird."

Im Maßnahmenkatalog werden die technischen Bedürfnisse im Sinne internationaler Interoperabilität (z.B. X.509-Zertifikate) weitgehend berücksichtigt.

Der Maßnahmenkatalog stellt die Bauanleitung für die Errichtung der Infrastruktur zum Einsatz digitaler Signaturen im Sinne des Signaturgesetzes dar.

Der Maßnahmenkatalog hat empfehlenden Charakter.

Nur, wenn ensprechend den Vorschlägen des Maßnahmenkatalogs vorgegangen wird, ist mit einer Lizenzierung/ Zertifizierung zu rechnen.

(1.3) Was fehlt?

Zitat

„Soweit durch Rechtsvorschrift die Schriftform vorgegeben ist, wird geprüft, ob und in welchen Fällen es zweckmäßig erscheint, neben der Schriftform auch die »digitale Form« mit digitaler Signatur zuzulassen."

Aus: Amtliche Begründung zum Regierungsentwurf des Signaturgesetzes

Die digitale Signatur kann die Unterschrift nur an manchen Stellen ersetzen. Bei vielen Rechtsgeschäften kann auf die »klassische« Unterschrift nicht verzichtet werden.

Unterschrift und digitale Signatur haben nicht dieselbe -rechtliche- Beweiskraft. Ein Urkundenbeweis ist mit einem digital signierten Dokument nicht zu führen.

Zitat

„Hinsichtlich der Haftung der Zertifizierungsstellen gegenüber Dritten kann sich im Einzelfall eine Haftungslücke ergeben."

Aus: Amtliche Begründung zum Regierungsentwurf des Signaturgesetzes

Weder Signaturgesetz, noch Signaturverordnung oder Maßnahmenkatalog klären die Haftungsfrage. Es bleibt offen, wer bei einem Schaden haftet, der z.B. trotz gesetzeskonformer Vorgehensweise, d.h. weder schuldhaft, noch fahrlässig, eintritt. Der Adressat eines digital signierten Dokuments trägt das Schadensrisiko allein. Konkret:

- *Produkthaftung* (ProdHaftG) trifft nur auf -gegenständliche- Produkte (und Strom) zu, nicht auf Dienstleistungen.
- *Vertragshaftung* (§§459, 634 BGB) gilt nur für Vertragspartner.
- *Produzentenhaftung* (§823 BGB) erstreckt sich nicht auf Vermögensschäden.
- *Staatshaftung* (Art. 34 GG) umschließt nur hoheitsrechtliche Handlungen der Behörde (hier: RegTP).

Außerdem: Die vorgesehenen Kontrollmöglichkeiten sind nicht geeignet, Transparenz zu schaffen und Anwendern Sicherheit zu geben.

(2) Einführung in die Kryptographie

(2.1) Meilensteine der historischen Entwicklung

Die Kryptographie ist ein Gebiet der Kryptologie. Sie befaßt sich mit der Geheimhaltung von Informationen. Das andere Gebiet der Kryptologie, die Krypt(o)analyse befaßt sich mit dem Lesbarmachen von verschlüsselten Informationen.

Bereits in der **Antike** werden Verschlüsselungen eingesetzt, z.B. die »Cäsar-Chiffrierung«, eine einfache Substitution.

In **Mittelalter und Renaissance** wird der geheime Nachrichtenaustausch in Geheimkabinetten gepflegt. Es kommen kompliziertere Substitutionen und Transpositionen zum Einsatz. Auch werden erste Codebücher benutzt.

Zur **Jahrhundertwende** etablieren sich Chiffrierwalzen, die später zu Rotormaschinen weiterentwickelt werden. Berühmtestes Beispiel ist die Enigma, die auf deutscher Seite zum Einsatz kam.

Nach dem zweiten Weltkrieg wird von Geheimdiensten intensiv auf kryptologischem Gebiet geforscht. Die Ergebnisse sind weitgehend unbekannt.

1975 wird die DES-Spezifikation im "Federal Register" der USA veröffentlicht. Erstmals wird so ein sicherer (symmetrischer) Verschlüsselungsalgorithmus öffentlich gemacht. DES markiert den Anfang öffentlicher Kryptographie.

1976 veröffentlichten W. Diffie und M. Hellman die grundlegende Idee für die asymmetrische Kryptographie (public key cryptography).

1978 (1977) wird das erste asymmetrische Verschlüsselungsverfahren (RSA) von seinen Entwickler R. Rivest , A. Shamir und L. Adleman vorgestellt. Das Verfahren wird 1978 patentiert.

Etwa zur gleichen Zeit (**Mitte der 70'er Jahre**) begannen intensive Forschungen über kryptographische Hashfunktionen.

1991 wird in den USA der Digital Signature Standard (DSS) vorgestellt.

1995 verabschiedet der Bundesstaat Utah in den USA das weltweit erste Gesetz über digitale Signaturen - den Utah Digital Signature Act (UDSA).

1996 (Dez.) verabschiedete der deutsche Bundestag das Signaturgesetz (SigG), das weltweit erste nationale Gesetz über digitale Signaturen. Das Gesetz tritt zum 1. August 1997 in Kraft.

1998 wird als erster internationaler Vertrag ein Abkommen zwischen Pennsylvania (USA), Kanada und Singapur digital signiert.

Nachtrag (vom 3.11.1998)

Mai 1998 Die Electronic Frontier Foundation (EFF) veröffentlicht das Buch "Cracking DES", in dem nachgewiesen wird, daß DES nicht sicher ist.

September 1998 Das NIST gibt bekannt, daß ein DES-Nachfolger gesucht wird.

Oktober 1998 Die oberste Zertifizierungsinstanz der BRD (gemäß SigG) ist arbeitsbereit und generiert ihre Schlüssel.

Oktober 1998 Acht internationale Großbanken, darunter die Deutsche Bank und die Hypovereinsbank, beschließen die Errichtung einer internationalen Zertifizierungsinfrastruktur, die nicht mit dem Signaturgesetz kompatibel ist.

(2.2) Symmetrische/asymmetrische Verschlüsselungsverfahren

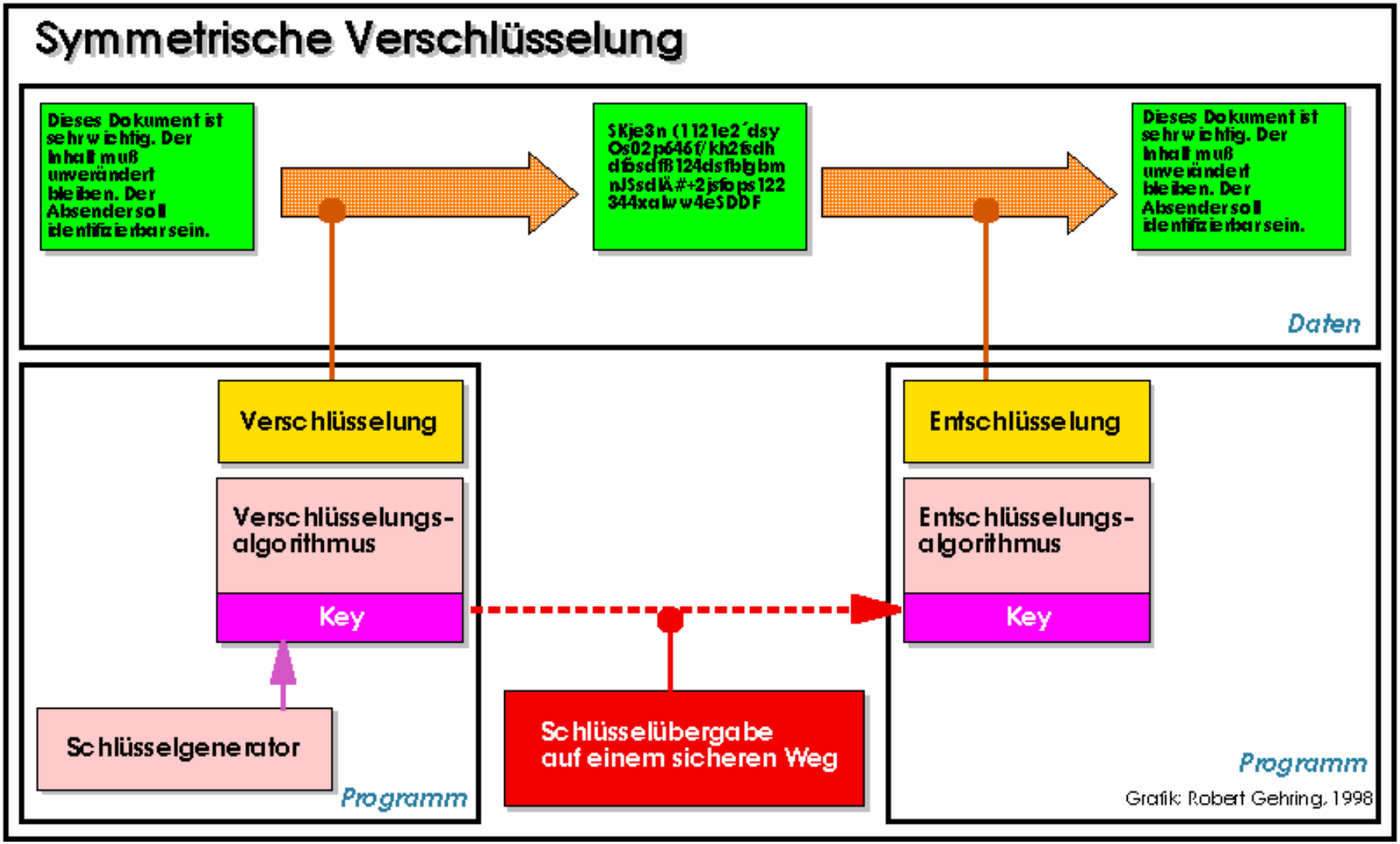
(2.2.1) Verschlüsselung/Entschlüsselung

- Als Verschlüsselung bezeichnet man die Umwandlung von Informationen in unverständliche, verschlüsselte Daten. Dazu dient ein Verschlüsselungsverfahren, sowie (oft) ein Schlüssel als steuernder Parameter.

- Entschlüsselung ist die Wiederherstellung der ursprünglichen Information aus den unverständlichen, verschlüsselten Daten. Das entsprechende Verfahren wird seinerseits (oft) durch einen Schlüssel gesteuert.

(2.2.2) Symmetrische Verschlüsselung

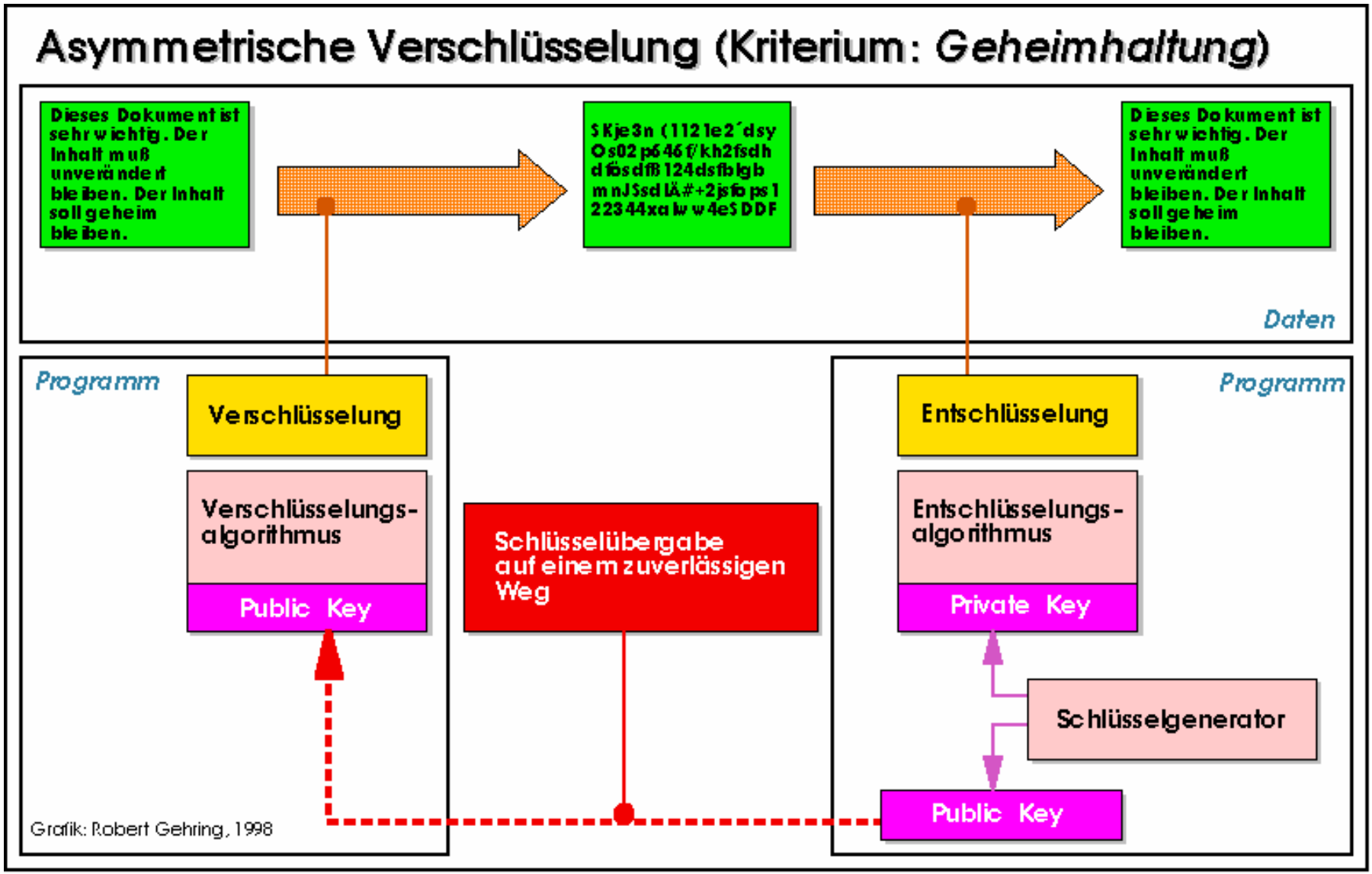
- Werden für die Steuerung der Ver- bzw. Entschlüsselung Kopien ein- und desselben Schlüssels eingesetzt, so spricht man von symmetrischer Verschlüsselung (private key encryption).



Erläuterung: Mit einem geeigneten Verfahren wird ein Schlüssel erzeugt. Von diesem Schlüssel muß eine Kopie jedem Kommunikationspartner zur Verfügung gestellt werden. Mit diesem Schlüssel kann eine Nachricht ver- und entschlüsselt werden. Um zu verhindern, daß Dritte unbefugt vom Inhalt einer verschlüsselten Nachricht Kenntnis erlangen können, muß sichergestellt werden, daß nur berechtigte Personen eine Schlüsselkopie erhalten. Wenn mehrere Personen über eine Schlüsselkopie verfügen (und mindestens zwei Personen sind es), ist eine Authentifizierung nicht möglich, da jeder Schlüsselkoipieinhaber eine Nachricht erzeugen und verschlüsseln kann.

(2.2.3) Asymmetrische Verschlüsselung

- Kommen zur Steuerung von Ver- und Entschlüsselung unterschiedliche Schlüssel zum Einsatz, so spricht man von asymmetrischer Verschlüsselung (public key encryption).



Erläuterung: Mit einem geeigneten Verfahren wird ein Paar asymmetrischer Schlüssel (privater Schlüssel, öffentlicher Schlüssel) generiert. Die besondere Eigenschaft dieser Schlüssel ist es, daß mit dem einen Schlüssel entschlüsselt werden kann, was mit dem anderen Schlüssel verschlüsselt wurde. Dabei ist es egal, mit welchem Schlüssel die Verschlüsselung vorgenommen wird. Nur die Schlüssel aus dem generierten Paar gestatten im Zusammenspiel die Ver- und Entschlüsselung.

Einer der Schlüssel aus dem Paar verbleibt beim Absender einer Nachricht (deshalb: privater Schlüssel), der andere wird dem/den Empfänger/Empfängern zur Verfügung gestellt (deshalb: öffentlicher Schlüssel). Diese Schritte werden von jedem Kommunikationsteilnehmer vollzogen, so daß alle am Ende über ein Unikat ihres privaten Schlüssels und über Kopien der öffentlichen Schlüssel der anderen verfügen.

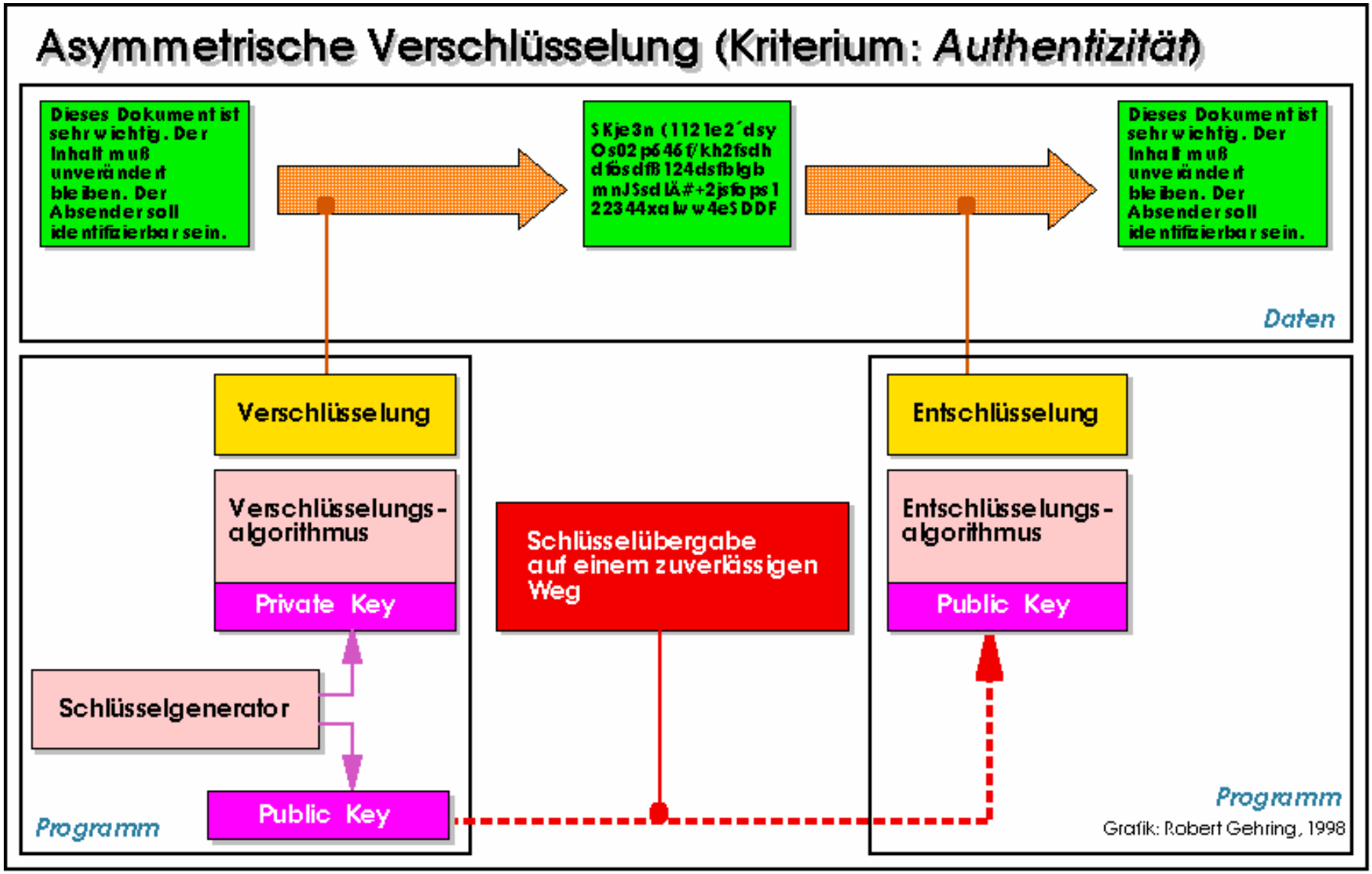
Damit lassen sich zwei Fälle unterscheiden:

(A) Geheimhaltung

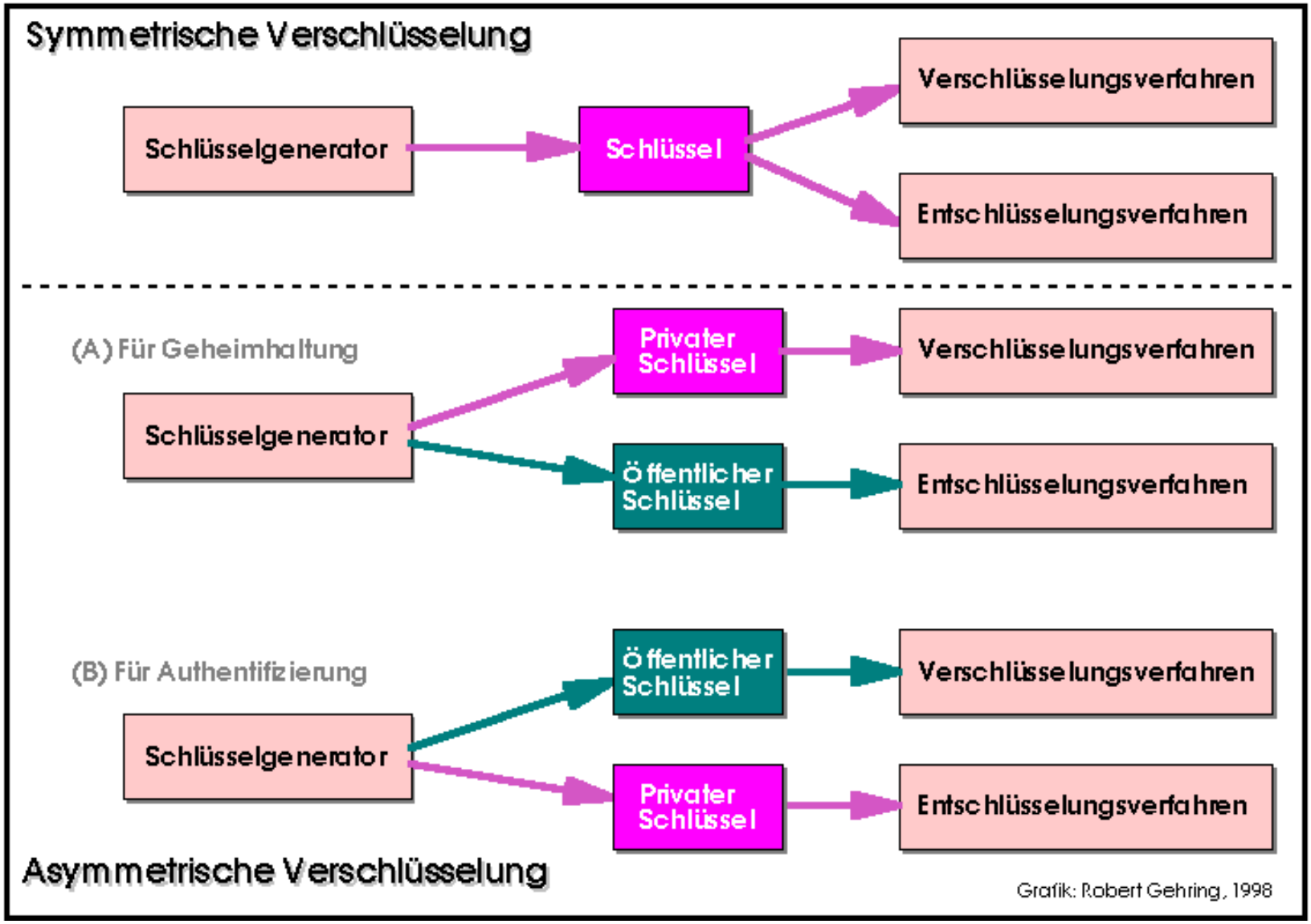
Ein Teilnehmer will einem Kommunikationspartner eine geheime Nachricht zukommen lassen. Da er über eine Kopie des öffentlichen Schlüssels des Partners verfügt, verschlüsselt er die Nachricht mit deren Hilfe. Da nur der Inhaber des zugehörigen privaten Schlüssels eine so verschlüsselte Nachricht wieder entschlüsseln kann, kann niemand anderes an den Inhalt der Nachricht gelangen, selbst wenn die Nachricht abgefangen werden sollte. Dieser Fall ist in der oberen Zeichnung dargestellt.

(B) Authentifizierung

Ein Teilnehmer verschlüsselt eine Nachricht mit seinem privaten Schlüssel. Dann kann jeder, der über eine Kopie des zugehörigen öffentlichen Schlüssels verfügt, die Nachricht entschlüsseln. Gelingt die Entschlüsselung, so weiß er, daß die Nachricht nur vom Inhaber des zu dem verwendeten öffentlichen passenden geheimen Schlüssels verschlüsselt worden sein kann. Daher muß die Nachricht authentisch sein. Dieser Fall ist unten dargestellt.



Gegenüberstellung von symmetrischer und asymmetrischer Kryptographie



(2.3) Daten- und Kommunikationssicherheit

(2.3.1) "Technische Sicherheit"

Moderne Verschlüsselungsverfahren bieten hohe Sicherheit bei guter Verfügbarkeit. Der technische Aufwand, eine solche Verschlüsselung zu brechen,

kann das Menschenmögliche übersteigen. Der technische Aufwand, Daten derartig zu verschlüsseln, ist dagegen bereits mit einem normal ausgestatteten PC zu realisieren.

Praktisch absolute Sicherheit ist *machbar*.

(2.3.2) "Politische Sicherheit"

Moderne Verschlüsselungsverfahren sind (vermutlich) für Geheimdienste nicht zu brechen. Informationen jeder Art können so gegen unbefugten Zugriff gesichert werden. Daraus entsteht ein Konflikt zwischen den Sicherheitsbedürfnissen der Anwender und denKontrollbedürfnissen der nationalen Sicherheitsbehörden.

Praktisch absolute Sicherheit ist *unerwünscht*.

(2.3.3) "Wirtschaftliche Sicherheit"

Ausländische Geheimdienste und konkurrierende Unternehmen sind an unsicheren Systemen interessiert, zu Spionagezwecken und zur Sabotage. (Beispiel: ECHELON-System) Solche Tätigkeiten stellen im Erfolgsfall eine reale Gefahr für die wirtschaftliche Überlebensfähigkeit eines Unternehmens dar.

Praktisch absolute Sicherheit ist *unverzichtbar*.

(2.3.4) "Private Sicherheit "

Private Kommunikation unter Verwendung elektronischer Medien wird immer selbstverständlicher. Der Schutz der privaten Kommunikation hat in Deutschland Verfassungsrang (GG Art.10).

Praktisch absolute Sicherheit ist ein *Verfassungrecht*.

(2.3.5) Fazit

Die Problematik der Daten- und Kommunikationssicherheit durch Verschlüsselung birgt *erhebliches Konfliktpotential*.

(3) Grundlagen und Konzepte digitaler Signaturen

(3.1) Grundbegriffe

(3.1.1) Integrität (integrity)

Eine Information behält ihre Integrität, wenn sie auf dem Weg von ihrer Quelle zu ihrem Empfänger unverändert bleibt.

(3.1.2) Identität (identity)

(a) Jeder Kommunikationsteilnehmer hat eine Identität.

(b) Durch eine digitale Signatur bekommt jede Information eine Identität.

(3.1.3) Authentifizierung (authentication)

Unter der Authentifizierung einer Information versteht man die Überprüfung der Identität der Information und ihrer Quelle. Dazu wird die Identität der Quelle benötigt.

Authentifizierung einer Person meint den Nachweis der behaupteten Identität der Person.

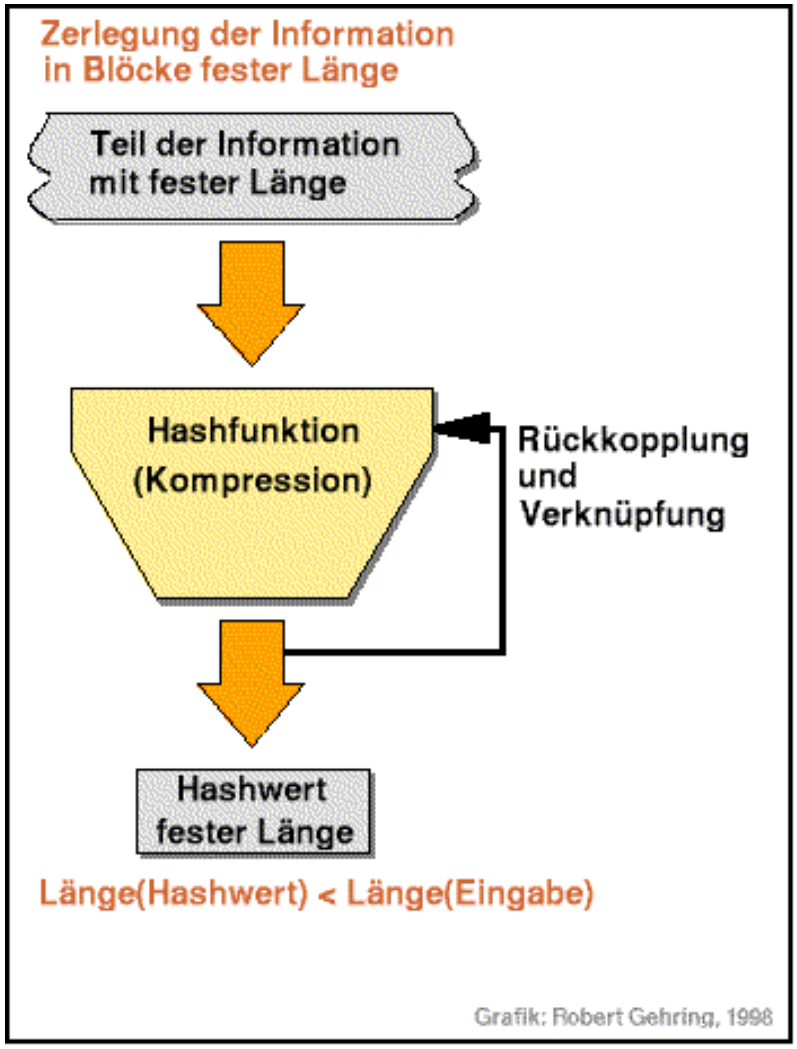
(3.1.4) Unabweisbarkeit (non-repudiation)

Eine Information hat die Eigenschaft der Unabweisbarkeit, wenn der Empfänger gegenüber Dritten der Quelle die Urheberschaft und die Integrität der Information nachweisen kann.

(3.2) Kryptographische Primitive

(3.2.1) Kryptographische Hashfunktionen

Kryptographische Hashfunktionen (mit und ohne Schlüssel) dienen dazu, unumkehrbar eine eindeutige Aussage fester Länge über eine Information (Hashwert) zu machen. Anhand dieser Aussage (message digest) kann die Integrität der Information überprüft werden.



Erläuterung: Zuerst wird die zu hashende Information in Blöcke passender Länge zerteilt. Sollte die Länge der Information kürzer sein, als für die Hashfunktion benötigt, wird sie durch Hinzufügen willkürlicher Zeichen

"verlängert". Jeder einzelne Block durchläuft dann die Hashfunktion und wird auf eine feste Länge komprimiert. So werden z.B. aus 512 Bytes (Zeichen) Information 128 Bytes (128 Zeichen) Hashwert erzeugt. Dieser resultierende Hashwert wird der Hashfunktion zusammen mit dem nächsten Informationsblock wieder zugeführt und mit dessen Hashwert verknüpft (z.B. durch XOR). Dieser Vorgang wird solange wiederholt, bis alle Blöcke der ursprünglichen Information abgearbeitet sind. Im Ergebnis erhält man einen einzelnen Hashwert, den sogenannten "message digest", auch "digitaler Fingerabdruck" genannt. Zu jeder Information, die eingegeben wird, erzeugt die Hashfunktionen einen anderen "Fingerabdruck".

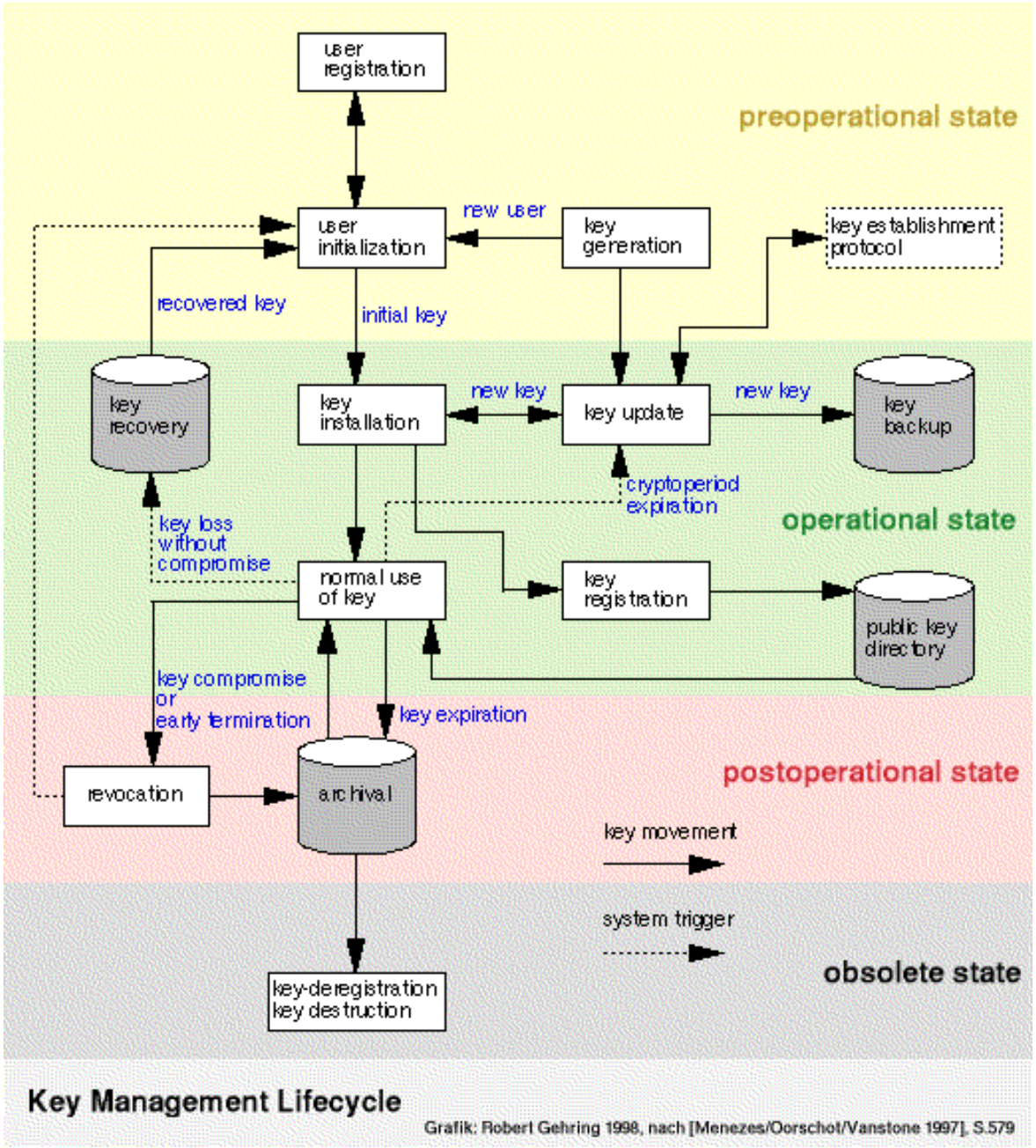
(3.2.2) Public Key-Verfahren

Public Key-Verfahren sind asymmetrische Verschlüsselungsverfahren. Durch die Verschlüsselung des Hashwertes einer Information mit dem privaten Schlüssel eines asymmetrischen Schlüsselpaares erhält die Information eine Identität. Wer über den öffentlichen Schlüssel aus dem Schlüsselpaar verfügt, kann diese Identität überprüfen.

(3.3) Schlüsselverwaltung, Zeit

Die Schlüsselverwaltung (key management) umfaßt alle Aktivitäten bezüglich der Schlüssel, die für eine verschlüsselte Kommunikation notwendig sind. Sichere Kommunikation hängt von sicheren Verschlüsselungsverfahren und einer sicheren Schlüsselverwaltung ab.

Die folgende Grafik gibt die wesentlichen Aspekte der Schlüsselverwaltung wieder.



Erläuterung: [Die Grafik wurde nach einem Bild aus dem Buch "Handbook of Applied Cryptography" von Menezes, van Oorschot und Vanstone (S.579) gestaltet. Die Autoren beziehen in ihrer Darstellung die Schlüsselerzeugung und Schlüsselvernichtung mit ein. In der Grafik wird eine "public key"-Infrastruktur beschrieben, zu erkennen am "public key directory".]

Jeder Anwender, der einen Schlüssel benutzen will (z.B. um digitale Signaturen zu erzeugen), identifiziert sich gegenüber dem System, in dem der Schlüssel zum Einsatz kommen soll (security domain). In der Regel wird er seine Schlüssel selbst generieren und registrieren lassen. Wenn nötig, wird der geheime Schlüssel auf einer Chipkarte o.ä. installiert. Eventuell wird der Schlüssel bereits auf einer Chipkarte generiert und verbleibt dort. In jedem Fall sind Maßnahmen zu ergreifen, die der Qualitätssicherung in Bezug auf Schlüssel und Verschlüsselungsverfahren dienen. Der öffentliche Schlüssel (public key) wird in einem öffentlichen Verzeichnis (public key directory) zugänglich gemacht.

Nach Ablauf des Zeitraumes, in dem die Sicherheit des Einsatz sowohl für den Schlüssel, als auch für das Verfahren gewährleistet ist, wird deren Einsatz unmöglich gemacht. Dazu kann der Schlüssel für ungültig erklärt oder auch zerstört werden. Alternativ wird das Verschlüsselungsverfahren aus dem Verkehr gezogen.

Wenn ein Schlüssel vor Ablauf dieses Zeitraumes als unsicher eingestuft werden muß, z.B. weil er kompromittiert, d.h. aufgedeckt wurde, wird er gesperrt. Diese Sperrung wird registriert und ggf. werden alle Betroffenen davon unterrichtet.

Solange Schlüssel und Verfahren nicht gesperrt sind, können sie zur Absicherung der Kommunikation eingesetzt werden. Unter Umständen ist es sinnvoll, Duplikate der Schlüssel an einem sicheren Ort aufzubewahren, um bei unabsichtlichem Verlust des Schlüssels Zugriff auf verschlüsseltes Material zu bekommen. (Man denke an Betriebsgeheimnisse. Sollten diese verschlüsselt worden sein, kann der Verlust des Schlüssels die Existenz gefährden.) Die Integration von "key recovery" in die Schlüsselverwaltung verringert jedoch die Sicherheit des Systems und eröffnet Mißbrauchsmöglichkeiten.

Viele Abläufe in der Schlüsselverwaltung sind zeitkritisch, z.B. die Bekanntgabe ungültig gewordener Schlüssel oder die Ersetzung unsicher gewordener Verschlüsselungsverfahren. Die Verfügbarkeit einer zuverlässigen Zeitangabe muß deshalb sichergestellt werden.

(3.4) Summa summarum: Die »digitale Signatur«

Kombiniert man auf geeignete Weise

- kryptographische **Hashfunktionen**

mit

- asymmetrischen **Verschlüsselungsverfahren**,

einer

- zuverlässigen **Schlüsselverwaltung**

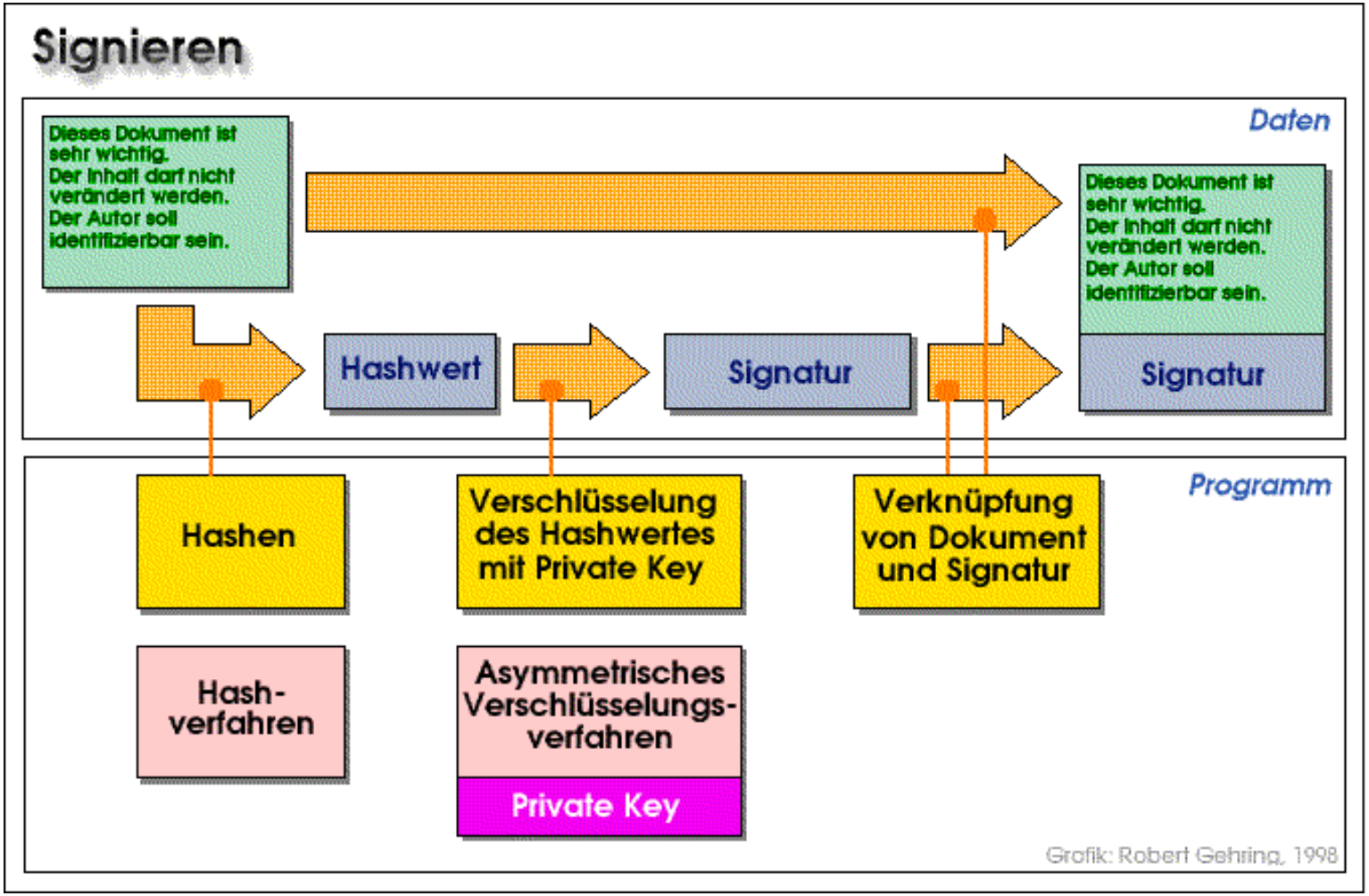
und einer

- geeigneten **Teilnehmeridentifizierung** (Zertifizierung),

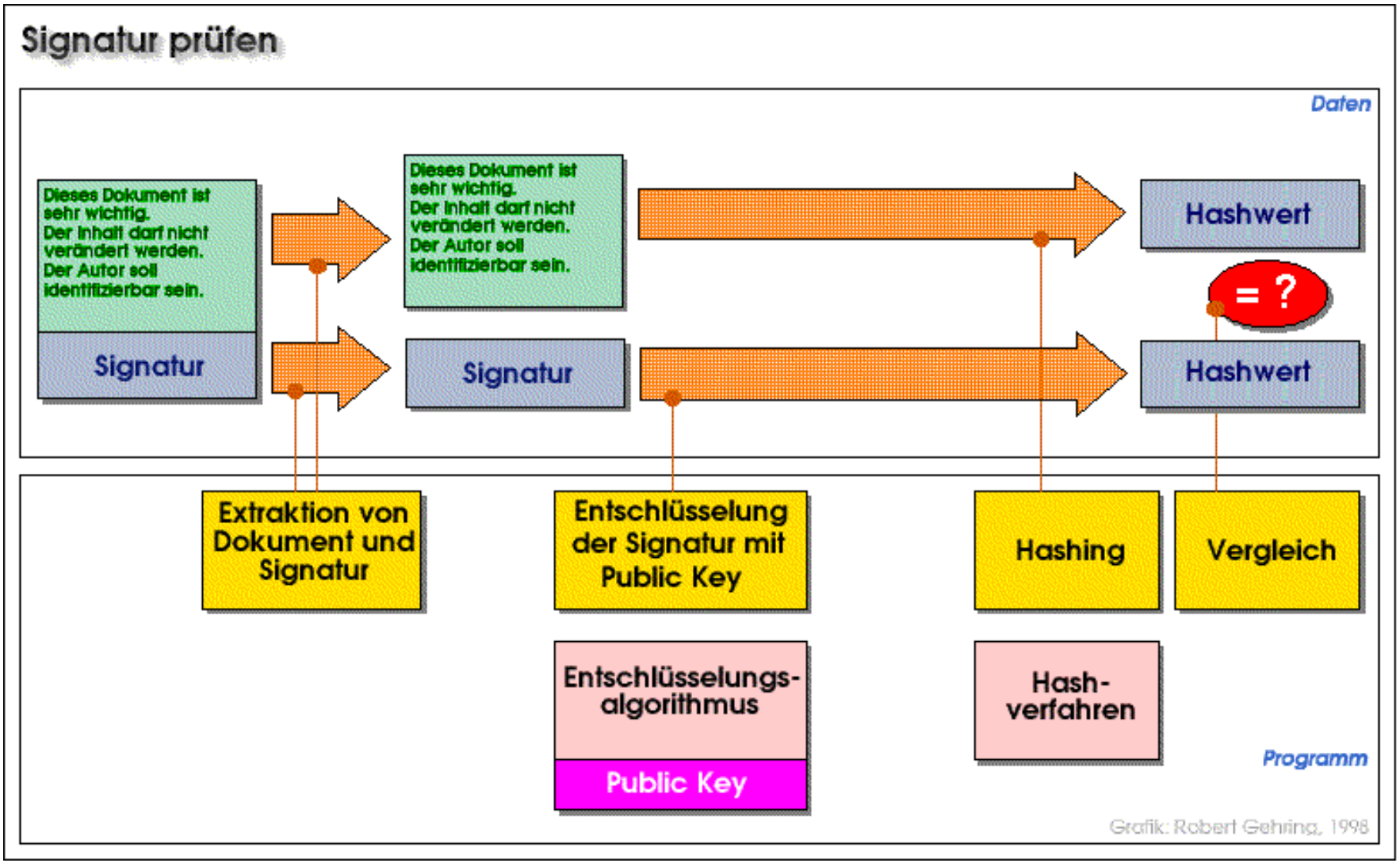
so erhält man

digitale Signaturen.

Der Einsatz digitaler Signaturen hat zwei Aspekte: Signaturen erzeugen und Signaturen prüfen.

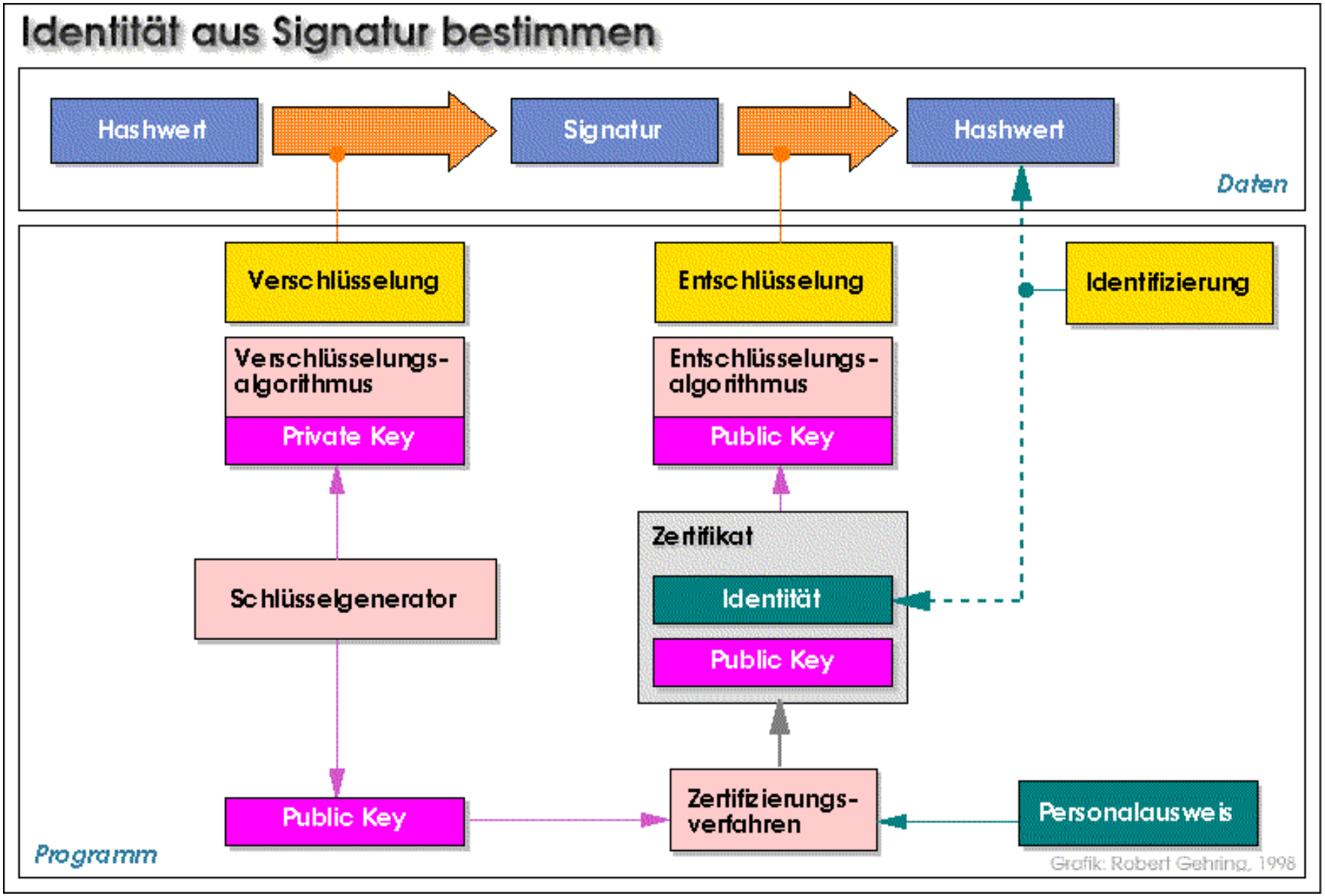


Erläuterung: Um eine Signatur zu erzeugen, wird das zu signierende Dokument durch eine kryptographische Hashfunktion komprimiert. Das Komprimat, der "message digest", wird anschließend mit einem asymmetrischen Verfahren verschlüsselt. Dazu wird der geheime Schlüssel (private key) aus dem asymmetrischen Schlüsselpaar benutzt. Im Ergebnis erhält man die Signatur des Dokuments, die mit dem Dokument verknüpft wird und ihm eine Identität verleiht.



Erläuterung: Um die Integrität eines empfangenen Dokuments zu prüfen, wird es in Signatur und Dokumenteninhalt zerlegt. Die Signatur wird mit Hilfe des öffentlichen Schlüssels des Absenders, den man z.B. dem Zertifikat für den Absender entnehmen kann, entschlüsselt. Dadurch erhält man die Hashmarke des ursprünglichen Dokuments. Der Dokumenteninhalt, von dem die Signatur abgetrennt wurde, wird mit demselben Hashverfahren komprimiert, das auch der Absender benutzt hat. Daraus resultiert der Hashwert des empfangenen Dokuments. Die beiden Hashwerte vergleicht man anschließend. Sind sie gleich, bedeutet das, daß der Inhalt des empfangenen Dokuments mit dem Inhalt des abgesandten, ursprünglichen Dokuments gleich ist. Der Absender des Dokumentes ist im Besitz des geheimen Schlüssels, der zum verwendeten öffentlichen Schlüssel gehört. Seine Identität

kann z.B. aus einem Zertifikat entnommen werden.



Erläuterung: Um seine (oder ihre) Identität erkennbar zu machen, muß der Besitzer (die Besitzerin) sich zuerst als Inhbaber (Inhaberin) des öffentlichen Schlüssels registrieren lassen. Diese Aufgabe übernehmen Zertifizierungsstellen. Dort wird ein Identitätsnachweis von einer registrierwilligen Person und ein Nachweis über den Schlüsselbesitz verlangt. Wenn beides erbracht wird, stellt die Zertifzierungsstelle ein Zertifikat aus, das Angaben zur Person und den öffentlichen Schlüssel beinhaltet. - Der Schlüsseltest kann z.B.

folgendermaßen vor sich gehen: Die Zertifizierungsstelle erzeugt eine einigermaßen große Zufallszahl und verschlüsselt diese mit dem vorgelegten öffentlichen Schlüssel. Dann bekommt der (die) vorgebliche Inhaber (Inhaberin) die Aufgabe, die verschlüsselte Zahl wieder zu entschlüsseln. Ist er (sie) im Besitz des passenden geheimen Schlüssels, gelingt das. - Das Zertifikat wird zum Abruf auf einem Server zur Verfügung gestellt.
Der Empfänger eines signierten Dokuments kann die Identität dann auf zwei Art und Weisen prüfen. Die erste Möglichkeit besteht darin, daß er über den öffentlichen Schlüssel des Absenders verfügt. Damit testet er die Signatur (s.o.) und wendet sich dann an die Zertifizierungsstelle. Auf deren Server befindet sich das Zertifikat, in dem der öffentliche Schlüssel eingetragen ist. Diesem Zertifikat kann er dann die notwendigen Angaben zur Person des Schlüsselinhabers entnehmen. Die zweite Möglichkeit sieht so aus, daß der Empfänger nicht über den öffentlichen Schlüssel verfügt, sondern den Namen der Person kennt. Zu diesem sucht er auf dem Server der Zertifizierungsstelle das Zertifikat und entnimmt daraus den öffentlichen Schlüssel. Mit diesem testet er die Signatur. Der Test verläuft nur dann erfolgreich, wenn die Signatur mit dem geheimen Schlüssel des Absenders erzeugt wurde.

Digitale Signaturen können unter sicheren Voraussetzungen in elektronischen Medien (u.a.) die Funktionen von Unterschriften übernehmen.

- Mit ihrer Hilfe kann dem Unterzeichner nachgewiesen werden, daß er ,,eigenhändig" ein vorliegendes Dokument ,, unterzeichnet" hat.
- Es kann nachgewiesen werden, daß die Signatur zum Dokument gehört.
- Es kann nachgewiesen werden, daß der Inhalt des Dokuments unverändert ist.
- Wenn eine Zeitmarkierung vorgesehen ist, kann nachgewiesen werden, daß das Dokument zu einem bestimmten Zeitpunkt unterzeichnet wurde.

Wenn außerdem technisch sichergestellt ist, daß das unterzeichnete Dokument vor der Unterzeichnung vollständig wahrgenommen wurde, erfüllen digitale Signaturen die rechtlichen Anforderungen an Unterschriften.


In Vorbereitung